What’s the most popular mobile web browser?
What’s the second most popular mobile web browser?
After Google Chrome, UC Browser is most popular mobile browser in world

The Alibaba Group company over the last couple of years has become No.2 mobile browser in the world and has consolidated its position as the No. 1 mobile browser in three most populous countries of Asia - China, India and Indonesia.
StatCounter Global Stats
Top 9 Mobile Browsers from Aug 2015 to July 2016

- Chrome: 35.85%
- UC Browser: 17.76%
- Safari: 17.71%
- Opera: 11.52%
- Android: 10.38%
- Samsung Internet: 2.51%
- IEMobile: 1.82%
- BlackBerry: 0.78%
- Nokia: 0.38%
- Other: 1.29%
BAT (Baidu Alibaba Tencent) Browsers

Baidu Browser
(百度浏览器)

UC Browser
(UC浏览器)

QQ Browser
(QQ浏览器)
Synergising Network Analysis Tradecraft

Network Tradecraft Advancement Team (NTAT)
Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop

* Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics
Technical analysis

- Reverse engineered Android & Windows versions
- Findings:
  - Found that each uses “easily decryptable” crypto (or sometimes no crypto) to transmit sensitive data
  - Found that most have insecure self-updating processes vulnerable to remote code execution
Kinds of sensitive data typically sent

- **Personally identifiable**
  - MAC address
  - IMEI
  - IMSI

- **Location**
  - GPS
  - Active wireless access point
  - In-range wireless access points

- **Activity**
  - Search keywords
  - URL of every http(s) page visited
  - Title of every https(s) page visited
“Easily decryptable” crypto

- Easily decryptable by reverse engineering the software
- Someone eavesdropping on network traffic can decrypt
- *E.g.*, naive “homebrew” crypto algorithms
- Symmetric crypto algorithms with hard-coded keys
- Asymmetric crypto with huge flaws
Example transmission (encrypted)

m90.!.Ä#Ù.GÚ}â.~%..7ÚÁC.\..S+xKû.,ý..%/@&..cq*.Í2äh:ÜÈ´Ü>ë..½.OL8."|..°±..¿ Ü.ôýî. ìi°._WB.p..dÄ·..–à»ØOZíÁn..Ìw.äb.!á.©Oà.&.J.É.ü7.5 w-.°,°.Ý$......0F .ß.§>.{$.CW[¿=.P.é.ôH.nÞóTnM,...ý.ÉÜ+.íPÝû..u!p.åCÉhii!×Ýiaë 1î³¿.Ð@h.«Ww.X .u,−W.â{.H9ù·.Äx#.S...©...x.¢$w...¾;ýdt©î.ôR.£{jÝ!T,ãsD~Ñö}.pOnJ$...M5É.ÅAc. ýâJç©.É©.}|JzÄa/Ý%jM.´È.ØN/r¾..çÃÁi|F−.G±:°iiS¢¬ǒǐk8i$^6.p.;V−é.YQì.ùŐ.y+Íf.. ý+V.##.5.Í−P.(져h..O±ç..O>v2−äµ&r×À..dđ.Åt.;.©°x.Ñi..x.÷ãǑ¢ã...O.Û¶.Át"i´ö ZX.].ÑBuù.Ì°f&cô.ÓïW.ÒÜK.ßæ.°.W.ò.¿ñi3−...ê]G.Trg.¶»fKKb.ª.Ý.W.B..B.oª.c#.ú ..ÃÍ.Ð..µê.+².2Å
How to decrypt this?

- Reverse engineer the software
- Symmetric crypto :(  
- Discover algorithm: homebrew XOR
- Discover the key: "b59e216a8067d108"
- Write a python script
Example transmission by UC Browser (encrypted)
Decrypted

bluesky.1.5.1.1.10?cache=3102618000&ka=&kb=e2e63e260805aea910e1c2ce02b05211&kc=3b5d366db90b1b60e22260a0278331f8v0000002e9952d46&firstpid=0501&bid=800&ver=5.5.10106.5&defaultbrowser=UCHTML.AssocFile.HTML&flashver=&hi=Intel(R) Core(TM) i5-4300U CPU @ 1.90GHz&0&VB3bb90c33-fc547c89&searchaddress=google&searchbar=google&searchquick=google&openurltab=0&showsearch=1&showextension=1&applyall=0&cloudspeed=0&autopage=0&autologin=0&theme_id=569&wallpaper_id=207&autoclearhistory=0&service=1&sis_fool=5.1.2600_SP3_x86&tch=0&ad_switch=10&lang=zh-CN
Example 2 encrypted

m90.... _ō.÷.y.]¢="ùûİü<.Oò+Dûxh..Ej.a]ż?;..u.Öá..7ò.p`ùPD·.O"c.ioÔ, $ Ä.Üm.−. ø.ɨN."$gÉ^ć<kp8äL½.XgEÇ\0in...Ü5.F|¢?i.a3..Ím5°.ëó....ü−Ö% 7a. `(þ/mXaYnÅS... Øø...ý.÷tėØ3'gy..j...B±È.ÀOBxä.Ü.8'ì½u]ũÎ3Ne.O³¿G.Ö|.+½.ñpJÈN.+V.huÚ.È~[ø.SG" QÌLp`Ñ!.Рf^4eaá.čls.ÈfdĐ> Öz−v/6K.ÁĐy9.yÈ~...yÍ5.þ.st·U.Ö´.dÄE[ňFÀ.ÎF²L..ýè th= zãé−;ē=\nL..ØÔÖ¾[+[ÊÔI.−p!!!'alrÖ.0..qJ©\9Uë..Ƞy.ýk·2Ng−DÚ5Á.ó%<qE.u.ÿ. ø.â.20.Ú½−n.Ô]uù.z.ø.ç.Å..ũú`ä (WäO.ş.yà#:?+YA9.p3.:.1!ö£−.XE.X.ð→1ð.ĐCT.5/¿ *ØHø~©P.ÉJ .L©Gq.``.0O9:.'ùûHÈG..úLC..İ.;.xöJ¶n, ao+/©.ÉZ.Ø..ÚN....| .È8.æ.p. 9−F.š`.Ôåæ®.ëXü.1©>W.Ş.X2Â.c..r, {.İ°.+i.y{.çáÀ..N®Ü,- _ùR%.E%upÍÈcf.7ù&.n... iH×È < P.ÖZdüNÝ1.».mu.È. 7aeÌî, Y.Tj×yóë&;}..á.á.y÷−...B.³.u[...].riw, .:èQ)W.e]ü..ÑóûU.ö$öm−ûÔ};ôÔ...@^b\...îâ%Élq,ÂQPò..i só..t....9iNÈφmMEÍbÉA.ytr.÷Sö. .q$.).Sy5Bî.Q.Xòû.İ^nEKØ.ôM."t» «.ZÀ3mAØ¶O
Example 2 decrypted

bluesky.1.25.1.1.7?cache=3766412000&ka=&kb=e2e63e260805aea910e1c2ce02b05211&
kc=3b5d366db90b1b60e22260a0278331f8v0000002e9952d46&firstpid=0501&bid=800&ve
r=5.5.10106.5&type=1&ssl=1&bandwidth=29.63&target_ip=64.106.20.27&redirect_s
tart=0&redirect_duration=0&dns_start=0&dns_duration=218&connect_start=218&co
nnect_duration=251&request_start=469&request_duration=916&response_start=138
5&response_duration=1&dom_start=1386&dom_duration=268&dom_interactive=234&do
m_content_load_start=1420&dom_content_load_duration=0&load_event_start=1654&
load_event_duration=26&t0=1385&t1=1719&t2=1719&t3=1420&total_requests=2&requ
ests_via_network=2&cloud_acceleration_enabled=0&average_of_request_duration=
809&average_of_t2_duration=859&private_data=host=www.cs.unm.edu|url=https://
www.cs.unm.edu/~jeffk/|lang=zh-CN
Baidu Browser

- RC4 key "HR2ER"
- AES key "h9YLQoINGWyOBYYk"
- XOR mask (0x2D382324), bit rotations
- Base64 encoding with nonstandard alphabet:

```
qogjOuCRNkf15p4SQ3LaMxGKZTdesvB6z_YPahMI9t80rJyHW1DEwFbc7nUVX2-
```

- Modified TEA crypto + non-standard block cipher mode, key "vb%,J^d@2B1l'Abn" (*)
- ...

Baidu Browser

Data leaks across Windows & Android versions

<table>
<thead>
<tr>
<th>Type</th>
<th>Data Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>MAC address, hard drive serial number, IMEI</td>
</tr>
<tr>
<td>Activity</td>
<td>Search terms, Full HTTP(S) URLs, HTML page titles</td>
</tr>
<tr>
<td>Location</td>
<td>GPS coordinates, in-range WiFi access points</td>
</tr>
</tbody>
</table>
UC Browser

- Homebrew XOR-based algorithm with various keys ("b59e216a8067d108", "e19237a3a933f7eb", "aa171021f9438cb2")
- XOR mask "\xe9\xb9\xe9\xb3\x81\x8e\x97\xa7"
- ...
## UC Browser

Data leaks across Windows & Android versions

<table>
<thead>
<tr>
<th>Type</th>
<th>Data Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>IMEI, IMSI, Hard drive serial number, base board serial number, file system volume number</td>
</tr>
<tr>
<td>Activity</td>
<td>Full HTTP(S) URLs, Search terms</td>
</tr>
</tbody>
</table>
QQ Browser

- RSA public key 245406417573740884710047745869965023463
QQ Browser

- To factor it, we built our own quantum computer
QQ Browser

- RSA public key 245406417573740884710047745869965023463

Prime factorization:

14119218591450688427 × 1738101977696486069 (2 distinct prime factors)
QQ Browser

- RSA public key 245406417573740884710047745869965023463

![Prime factorization result](image)

- Also same peculiar TEA crypto as Baidu Browser (*)
- …
QQ Browser

Data leaks across Windows & Android versions

<table>
<thead>
<tr>
<th>Type</th>
<th>Data Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>PII</td>
<td>Machine hostname, Gateway MAC address, Hard drive serial number, Windows user security identifier, IMEI, IMSI, Android ID, QQ username, WiFi MAC address</td>
</tr>
<tr>
<td>Activity</td>
<td>Search terms, Full HTTP(S) URLs</td>
</tr>
<tr>
<td>Location</td>
<td>In-range WiFi access points, Active WiFi access point</td>
</tr>
</tbody>
</table>
Vulnerable SDK

- Code leaking personally identifying and locational data in browser actually from a Baidu SDK
- Found SDK in hundreds of Google Play store apps (some very popular)
- ES File Explorer File Manager (com.estrongs.android.pop) has 100,000,000 – 500,000,000 installs
- Other browsers have SDKs?
Vulnerabilities in update processes

- Remote code execution
- Vulnerabilities
  - Failing to check digital signatures (or protected with easily decryptable crypto)
    - Baidu Android, Baidu Windows, QQ Android, UC Windows
  - Failing to check version numbers → downgrade to vulnerable version
    - QQ Windows
  - Failing to check app name → sidegrade to vulnerable product
    - QQ Windows, UC Android
Success Stories

* UCWeb mobile browser identification
  * Discovered by GCHQ analyst during DSD workshop

* Chinese mobile web browser – leaks IMSI, MSISDN, IMEI and device characteristics
<table>
<thead>
<tr>
<th>State</th>
<th>ID</th>
<th>Date/Time Start</th>
<th>Date/Time End</th>
<th>Browser Version</th>
<th>Email Address</th>
<th>Handset Model</th>
<th>BMEl</th>
<th>BSEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2012-05-13 02:29:20</td>
<td>2012-05-13 02:29:23</td>
<td>8.0.3.107</td>
<td>212movies</td>
<td>nokiae90-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2012-05-13 06:00:59</td>
<td>2012-05-13 06:01:00</td>
<td>8.0.3.107</td>
<td>212movies</td>
<td>nokiae90-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>2012-05-14 12:29:53</td>
<td>2012-05-14 12:29:53</td>
<td>8.0.4.121</td>
<td></td>
<td>digol</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>2012-05-14 17:46:46</td>
<td>2012-05-14 17:46:46</td>
<td>8.0.4.121</td>
<td></td>
<td>nokiaE72-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Z</td>
<td>2012-05-15 20:02:56</td>
<td>2012-05-15 20:02:56</td>
<td>8.0.4.121</td>
<td></td>
<td>nokiaX6-00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Global Title: 9379900100
Platform: java
Active User: E9DLH.000000M0000
(S//SI//REL TO USA, FVEY) The CONVERGENCE team helped discover an active communication channel originating from the [redacted] that is associated with the [redacted], as they are known within the [redacted] hierarchy. The area of responsibility is for covert activities in Europe, North America, and South America. The customer [redacted] leveraged a **Convergence Discovery capability that enabled the discovery of a covert channel associated with smart phone browser activity in passive collection**. The covert channel originates from users who use UCBrowser (mobile phone compact web browser). The covert channel leaks the IMSI, MSISDN, Device Characteristics, and IMEI back to server(s) in [redacted]. Initial investigation has determined that perhaps malware can be associated with the covert channel is established. This covert exfil activity identifies SIGINT opportunity where potentially none may have existed before. Target offices that have access to X-KEYSCORE can search within this type of traffic based on their IMSI or IMEI to determine target presence.
Responsible Disclosure

Difficulties in submitting

Different conceptions of PII

Whac-a-mole
Why were there such similarities?

- Recall: the kinds of sensitive data leaked look very similar
- In one case, identically peculiar crypto algorithm

Market Factors

- Highly competitive market
- Collect it all
- Buying a (vulnerability) ecosystem
Why the similarities?

Political factors

- Lack of access to Google Play
- Chinese regulatory pressures
  - 2015 anti-terrorism law
  - Network security offices
Takeaways

- Security researchers should pay more attention to these understudied apps
- Huge user bases + major vulnerabilities = opportunity for user benefit
- Finding vulnerabilities in popular browsers is becoming increasingly difficult
- Any researcher that even looked at this traffic in Wireshark would know there is a problem
- We need to better engage with these companies and put pressure on them to design better products
Acknowledgments

This material is based upon work supported by the U.S. National Science Foundation under Grant Nos. #1420716 and #1518878. Jeffrey Knockel’s research for this project was supported by the Open Technology Fund’s Information Control Fellowship Program. Adam Senft’s research for this project was supported by the John D. and Catherine T. MacArthur Foundation (Ronald J. Deibert, Principal Investigator). The authors would like to thank Seth Hardy, Masashi Crete-Nishihata, Andrew Hilts, Sarah McKune, and Jason Q. Ng for assisting with this research.
Questions?